PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 527 di venerdì 29 marzo 2002

In circolazione una falsa patch di Microsoft

Il messaggio individuato non viene riconosciuto dai piu' diffusi programmi antivirus.

E' in circolazione un messaggio di posta elettronica che invita i destinatari a scaricare una falsa patch dal sito di Microsoft.

La pagina Web alla quale gli utenti vengono indirizzati è simile alle pagine del sito di Microsoft e fino a qualche giorno fa era raggiungibile anche attraverso l'indirizzo syntax.at/microsoft attualmente non più attivo.

Le segnalazioni del messaggio "sospetto" sono giunte a un noto quotidiano, che si occupa di sicurezza informatica, da parte di alcuni lettori e il file "patch.exe" che si dovrebbe scaricare non è stato rilevato da nessuno dei più diffusi antivirus disponibili sul mercato.

"Patch.exe" ha le dimensioni di circa 1 MB e, una volta lanciato, installa in Windows file e directory e in automatico cerca di attivare una connessione a ircd.mircx.com, un sito che cerca poi di raggiungere il client IRC.

Gli esperti pensano che gli eseguibili necessari per l'attivazione di questa connessione facciano parte di un tool controllabile da remoto, al quale i cracker, attraverso IRC, possono inviare informazioni e prelevare dati.

---

www.puntosicuro.it